CLAIMS

What is claimed is:

1. A method for a first device and a second device to maintain synchronization of a shared, dynamic secret, the method comprising:

the second device sending an authentication request to the first device;

the first device, in response to the authentication request,

authenticating the second device,

sending an authentication reply to the second device, and

advancing a first copy of the secret;

the second device, in response to the authentication reply,

advancing a second copy of the secret;

the first device,

sending data to the second device,

again advancing the first copy of the secret, and

sending a data completion message to the second device;

the second device,

consuming the data, and

in response to the data completion message, again advancing the second copy of the secret.

2. The method of claim 1 wherein the first device comprises a server and the second device comprises a web appliance.

3. The method of claim 1 further comprising:

the first device storing the again advanced first copy of the secret; and

the second device storing the again advanced second copy of the secret.

4. The method of claim 1 further comprising:

executing a recovery technique in response to the first and second copies of the secret becoming out of synchronization.

5. A system for use on a network, the system comprising:

a server including,

a communication interface,

a processor for performing logic operations,

storage,

stored in the storage, a first copy of a secret,

a secret validator, and

means for advancing the first copy of the secret;

a web appliance including,

a communication interface coupling the web appliance to the server over the network,

a processor for performing logic operations,

storage,

stored in the storage of the web appliance, a second copy of the secret,

means for advancing the second copy of the secret; and

the server and the web appliance further including,

a protocol for recovering synchronization of the first and second copies of the secret.

6. The system of claim 5 wherein the secret comprises a PIN.

7. The system of claim 6 wherein the PIN comprises a number of at least 80 bits.

8. A method for a client device to maintain synchronization of a first copy of a secret stored on the client device with a second copy of the secret stored on a server device, the method comprising the client device:

sending an authorization request to the server device;

in response to receiving from the server device an authentication reply,

advancing the first copy of the secret; and

in response to receiving data from the server device,

consuming the data, and

again advancing the first copy of the secret.

9. The method of claim 8 further comprising the client device:

in response to receiving data from the server device,

storing the again advanced first copy of the secret.

10. The method of claim 8 further comprising the client device:

in response to not receiving an affirmative authentication reply from the server device,

(a) advancing the first copy of the secret,

(b) sending the advanced first copy of the secret to the server device.

11. The method of claim 10 wherein the (a) advancing the first copy of the secret comprises twice advancing the first copy of the secret.

12. A method for a server to authenticate an appliance that is in communication with the server, the method comprising the server:

receiving from the appliance an authentication request;

sending an authentication reply to the appliance;

advancing a first copy of a secret stored on the server;

sending data to the appliance;

sending a data completion message to the appliance;

again advancing the first copy of the secret; and

storing the again advanced first copy of the secret on the server.

13. The method of claim 12 wherein the secret is a PIN.

14. The method of claim 12 wherein the secret comprises a value of at least 80 bits.

15. The method of claim 12 further comprising:

determining that the appliance is not authentic and, responsive to that determination,

logging the authentication request, and

disconnecting communication to the appliance.

16. An article of manufacture comprising:

a machine-accessible medium including instructions that, when accessed by a machine, cause the machine to perform the method of claim 8.

17. The article of manufacture of claim 16 further comprising:

instructions that, when accessed by the machine, cause the machine to perform the method of claim 10.

18. An article of manufacture comprising:

a machine-accessible medium including instructions that, when accessed by a machine, cause the machine to perform the method of claim 12.

19. The article of manufacture of claim 18 further comprising:

instructions that, when accessed by the machine, cause the machine to perform the method of claim 15.